



# Overview

---

This chapter provides these topics about the Catalyst 3550 multilayer switch software:

- [Features, page 1-1](#)
- [Management Options, page 1-6](#)
- [Network Configuration Examples, page 1-8](#)

## Features

The Catalyst 3550 software supports the hardware listed in the release notes. [Table 1-1](#) describes the features supported in this release.

**Table 1-1** *Features*

---

### Ease of Use and Ease of Deployment

---

- Cluster Management Suite (CMS) software for simplifying switch and switch cluster management through a web browser, such as Netscape Communicator or Microsoft Internet Explorer, from anywhere in your intranet
- Switch clustering technology, in conjunction with CMS, for
  - Unified configuration, monitoring, authentication, and software upgrade of multiple switches (refer to the release notes for a list of eligible cluster members).
  - Automatic discovery of candidate switches and creation of clusters of up to 16 switches that can be managed through a single IP address.
  - Extended discovery of cluster candidates that are not directly connected to the command switch.
- Hot Standby Router Protocol (HSRP) for command-switch redundancy

**Note** See the [“Advantages of Using CMS and Clustering Switches”](#) section on page 1-7. Refer to the release notes for the CMS and cluster hardware, software, and browser requirements.

---

**Table 1-1 Features (continued)****Performance Enhancement**

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports for optimizing bandwidth
- IEEE 802.3x flow control on all Ethernet ports
- EtherChannel for enhanced fault tolerance and for providing up to 8 Gbps (Gigabit EtherChannel) full duplex of bandwidth between switches, routers, and servers
- Port Aggregation Protocol (PAgP) for automatic creation of EtherChannel links
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown unicast and multicast traffic
- Cisco Group Management Protocol (CGMP) server support and Internet Group Management Protocol (IGMP) snooping for IGMP versions 1 and 2:
  - (For CGMP devices) CGMP for limiting multicast traffic to specified end stations and reducing overall network traffic
  - (For IGMP devices) IGMP snooping for limiting flooding of multicast traffic
- Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons
- System Database Management (SDM) templates for allocating system resources to maximize support for user-selected features

**Manageability**

- Dynamic Host Configuration Protocol (DHCP) for automating configuration of switch information (such as IP address, default gateway, host name, and Domain Name System [DNS] and Trivial File Transfer Protocol [TFTP] server names)
- Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding host name and to a TFTP server for administering software upgrades from a TFTP server
- Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding Media Access Control (MAC) address
- Cisco Discovery Protocol (CDP) versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network
- Network Time Protocol (NTP) for providing a consistent timestamp to all switches from an external source
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch uses
- In-band management access through CMS
- In-band management access through up to 16 simultaneous Telnet connections for multiple command-line interface (CLI)-based sessions over the network
- In-band management access through Simple Network Management Protocol (SNMP) versions 1 and 2c get and set requests
- Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem

**Note** For additional descriptions of the management interfaces, see the [“Management Options” section on page 1-6](#).

**Table 1-1 Features (continued)**

---

**Redundancy**

---

- Hot Standby Router Protocol (HSRP) for command switch and Layer 3 router redundancy
- UniDirectional Link Detection (UDLD) on all Ethernet ports for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
- IEEE 802.1d Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:
  - Per-VLAN Spanning Tree (PVST) for balancing load across virtual LANs (VLANs)
  - Port Fast mode for eliminating forward delay by enabling a port to immediately change from a blocking state to a forwarding state
  - UplinkFast, cross-stack UplinkFast, and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks and cross-stack Gigabit uplinks
  - STP root guard for preventing switches outside the core of the network from becoming the STP root

**Note** The switch supports up to 128 instances of STP.

---

**VLAN Support**

---

- Support for up to 1005 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
  - VLAN Membership Policy Server (VMPS) and VLAN Query Protocol (VQP) for dynamic VLAN membership
  - Inter-Switch Link (ISL) and IEEE 802.1Q trunking encapsulation on all ports for simplified network moves, adds, and changes; better management and control of broadcast and multicast traffic; and improved network security by establishing VLAN groups for high-security users and network resources
  - Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (802.1Q or ISL) to be used
  - VLAN Trunk Protocol (VTP) and VTP pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic
-

Table 1-1 Features (continued)

**Security**

- Password-protected access (read-only and read-write access) to management interfaces (CMS and CLI) for protection against unauthorized configuration changes
- Multilevel security for a choice of security level, notification, and resulting actions
- Static MAC addressing for ensuring security
- Protected port option for restricting the forwarding of traffic to designated ports on the same switch
- Bridge Protocol Data Unit (BPDU) Guard for shutting down a Port Fast-configured port when an invalid configuration occurs
- Standard and extended IP access control lists (ACLs) for defining security policies on routed interfaces
- VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/User Datagram Protocol (UDP) headers
- Source and destination MAC-based ACLs for filtering non-IP traffic
- Terminal Access Controller Access Control System Plus (TACACS+), a proprietary feature for managing network security through a TACACS server

**Quality of Service and Class of Service****Classification**

- IP type-of-service/Differentiated Services Code Point (IP TOS/DSCP) and class of service (CoS) marking priorities on a per-port basis for protecting the performance of mission-critical applications
- Flow-based packet classification (classification based on information in the MAC, IP, and TCP/UDP headers) for high-performance quality of service at the network edge, allowing for differentiated service levels for different types of network traffic and for prioritizing mission-critical traffic in the network

**Policing**

- Traffic-policing policies on the switch port for managing how much of the port bandwidth should be allocated to a specific traffic flow
- Aggregate policing for policing traffic flows in aggregate to restrict specific applications or traffic flows to metered, predefined rates
- Up to 128 policers on ingress ports  
Up to eight policers per egress port

**Out-of-Profile**

- Out-of-profile markdown for packets that exceed bandwidth utilization limits

**Egress Policing and Scheduling of Egress Queues**

- Four egress queues on all switch ports. These four queues can be configured with the Weighted Round Robin (WRR) scheduling algorithm.
- Tail drop and Weight Random Early Detection (WRED) techniques for avoiding congestion

**Table 1-1 Features (continued)**

---

**Layer 3 Support**

---

- Hot Standby Router Protocol (HSRP) for Layer 3 router redundancy
  - IP routing protocols for load balancing and for constructing scalable, routed backbones:
    - Routing Information Protocol (RIP) versions 1 and 2
    - Open Shortest Path First (OSPF)
    - Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP)
  - IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
  - Fallback bridging for forwarding non-IP traffic between two or more VLANs
  - Static IP routing for manually building a routing table of network path information
  - Equal-cost routing for load balancing and redundancy
  - Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and router solicitation messages to discover the addresses of routers on directly attached subnets
  - Protocol-Independent Multicast (PIM) for multicast routing within the network, allowing for devices in the network to receive the multicast feed requested and for switches not participating in the multicast to be pruned. Includes support for PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode.
  - Distance Vector Multicast Routing Protocol (DVMRP) tunnelling for interconnecting two multicast-enabled networks across non-multicast networks
  - DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients
- 

**Monitoring**

---

- Switch LEDs that provide visual management of port- and switch-level status
  - Four groups (history, statistics, alarm, and events) of embedded remote monitoring (RMON) agents for network monitoring and traffic analysis
  - Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
-

# Management Options

The Catalyst 3550 switch is designed for plug-and-play operation: you only need to configure basic IP information for the switch and connect it to the other devices in your network. If you have specific network needs, you can configure and monitor the switch—on an individual basis or as part of a switch cluster—through its various management interfaces.

## Management Interface Options

You can configure and monitor individual switches and switch clusters by using these interfaces:

- **CMS**—CMS is a graphical user interface that can be launched from anywhere in your network through a web browser such as Netscape Communicator or Microsoft Internet Explorer. CMS is already installed on the switch. Using CMS, you can fully configure and monitor a standalone switch, a specific cluster member, or an entire switch cluster. You can also display network topologies to gather link information and to display switch images to modify switch- and port-level settings.

For more information about CMS, see [Chapter 3, “Getting Started with CMS.”](#)

- **CLI**—The switch IOS CLI software is enhanced to support desktop- and multilayer-switching features. You can fully configure and monitor the switch and switch cluster members from the CLI. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station.

For more information about the CLI, see [Chapter 2, “Using the Command-Line Interface.”](#)

- **SNMP**—SNMP provides a means to monitor and control the switch and switch cluster members. You can manage switch configuration settings, performance, security, and collect statistics by using SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView.

You can manage the switch from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The switch supports a comprehensive set of MIB extensions and four RMON groups.

For more information about using SNMP, see [Chapter 16, “Configuring SNMP.”](#)

## Advantages of Using CMS and Clustering Switches

Using CMS and switch clusters can simplify and minimize your configuration and monitoring tasks. You can use Cisco switch clustering technology to manage up to 16 interconnected, supported Catalyst switches through one IP address. This can conserve IP addresses if you have a limited number of them. CMS is the easiest interface to use and makes switch and switch cluster management accessible to authorized users from any PC on your network.

By using switch clusters and CMS, you can

- Manage and monitor interconnected Catalyst switches (refer to the release notes for a list of supported switches), regardless of their geographic proximity and interconnection media, including Ethernet, Fast Ethernet, Fast EtherChannel, Cisco GigaStack Gigabit Interface Converter (GBIC), Gigabit Ethernet, and Gigabit EtherChannel connections.
- Accomplish multiple configuration tasks from a single CMS window without needing to remember CLI commands to accomplish specific tasks.
- Apply actions from CMS to multiple ports and multiple switches at the same time. Here are some examples of configuring and managing multiple ports and switches:
  - Port configuration such as speed and duplex settings
  - Port and console port security
  - NTP, STP, VLAN, and QoS configuration
  - Inventory and statistic reporting and link- and switch-level monitoring and troubleshooting
  - Group software upgrade
- View a topology of interconnected devices to identify existing switch clusters and eligible switches that can join a cluster. You can also use the topology to quickly identify link information between switches.
- Monitor real-time status of a switch or multiple switches from the LEDs on the front-panel images. The system, redundant power system (RPS), and port LED colors on the images are similar to those used on the physical LEDs themselves.
- Use an interactive mode that takes you step-by-step through configuring complex, Layer 3 features such as:
  - ACLs
  - QoS
  - IP routing
  - Router redundancy
- Use wizards that prompt you to provide only minimal required information to configure these features:
  - QoS priorities on ports so that they give high priority to video traffic
  - IP multicast routing on a device so that it can forward multicast packets as a part of a multicast tree

For more information about CMS, see [Chapter 3, “Getting Started with CMS.”](#) For more information about switch clusters, see [Chapter 5, “Clustering Switches.”](#)

# Network Configuration Examples

This section provides network configuration concepts and includes examples of using the switch in different network topologies.

## Design Concepts

As your network users compete for network bandwidth, it takes longer to send and receive data. When you configure your network, consider the bandwidth required by your network users and the relative priority of the network applications they use.

[Table 1-2](#) describes what can cause network performance to degrade and describes how you can configure your network to increase the bandwidth available to your network users.

**Table 1-2** *Increasing Network Performance*

Network Demands	Suggested Design Methods
Too many users on a single network segment and a growing number of users accessing the Internet	<ul style="list-style-type: none"> <li>• Create smaller network segments so that fewer users share the bandwidth, and use VLANs and IP subnets to place the network resources in the same logical network as the users who access those resources most.</li> <li>• Use full-duplex operation between the switch and its connected workstations.</li> </ul>
<ul style="list-style-type: none"> <li>• Increased power of new PCs, workstations, and servers</li> <li>• High bandwidth demand from networked applications (such as e-mail with large attached files) and from bandwidth-intensive applications (such as multimedia)</li> </ul>	<ul style="list-style-type: none"> <li>• Connect global resources—such as servers and routers to which network users require equal access—directly to the high-speed switch ports so that they have their own high-speed segment.</li> <li>• Use the EtherChannel feature between the switch and its connected servers and routers.</li> </ul>

Bandwidth alone is not the only consideration when designing your network. As your network traffic profiles evolve, consider providing network services that can support applications for voice and data integration, multimedia integration, application prioritization, and security. [Table 1-3](#) describes some network demands and how you can meet those demands.

**Table 1-3 Providing Network Services**

Network Demands	Suggested Design Methods
Efficient bandwidth usage for multimedia applications and guaranteed bandwidth for critical applications	<ul style="list-style-type: none"> <li>• Use IGMP snooping to efficiently forward multimedia and multicast traffic.</li> <li>• Use other QoS mechanisms such as packet classification, marking, scheduling, and congestion avoidance to classify traffic with the appropriate priority level, thereby providing maximum flexibility and support for mission-critical, unicast, and multicast and multimedia applications.</li> <li>• Use optional IP multicast routing to design networks better suited for multicast traffic.</li> <li>• Use MVR to continuously send multicast streams in a multicast VLAN, but to isolate the streams from subscriber VLANs for bandwidth and security reasons.</li> </ul>
High demand on network redundancy to provide <i>always on</i> mission-critical applications	<ul style="list-style-type: none"> <li>• Use HSRP for router redundancy.</li> <li>• Use VLAN trunks, cross-stack UplinkFast, and BackboneFast for traffic-load balancing on the uplink ports so that the uplink port with a lower relative port cost is selected to carry the VLAN traffic.</li> </ul>
An evolving demand for IP telephony	<ul style="list-style-type: none"> <li>• Use QoS to prioritize applications such as IP telephony during congestion and to help control both delay and jitter within the network.</li> <li>• Use switches that support at least two queues per port to prioritize voice and data traffic as either high- or low-priority, based on 802.1p/Q.</li> <li>• Use voice VLANs (VVIDs) on the Catalyst 2900 XL and Catalyst 3500 XL switches to provide separate VLANs for voice traffic.</li> </ul>
A growing demand for using existing infrastructure to transport data and voice from a home or office to the Internet or an intranet at higher speeds	<p>Use the Catalyst 2900 LRE XL switches to provide up to 15 Mb of IP connectivity over existing infrastructure, such as existing telephone lines.</p> <p><b>Note</b> Long-Reach Ethernet (LRE) is the technology used in the Catalyst 2900 LRE XL switches. Refer to the Catalyst 2900 XL and Catalyst 3500 XL documentation set about these switches and the LRE technology.</p>

Figure 1-1 shows three configuration examples for using Catalyst switches to create the following:

- **Cost-effective wiring closet**—A cost-effective way to connect many users to the wiring closet is to connect a Catalyst switch cluster of up to nine Catalyst 3500 XL switches (or with a mix of Catalyst 2900 XL and Catalyst 3500 XL switches) through GigaStack GBIC connections. To preserve switch connectivity if one switch in the stack fails, connect the bottom switch to the top switch to create a GigaStack loopback and enable cross-stack UplinkFast on the cross-stack Gigabit uplinks.

You can have redundant uplink connections, using Gigabit GBIC modules, from the GigaStack cluster to a Gigabit backbone switch such as the Catalyst 3550-12T switch. You can also create backup paths by using Fast Ethernet, Gigabit, or EtherChannel links. If one of the redundant connections fails, the other can serve as a backup path. You can configure the stack members and the Catalyst 3550-12T switch as a switch cluster to manage them through a single IP address. The Catalyst 3550-12T switch can be connected to a Gigabit server through a 1000BASE-T connection.

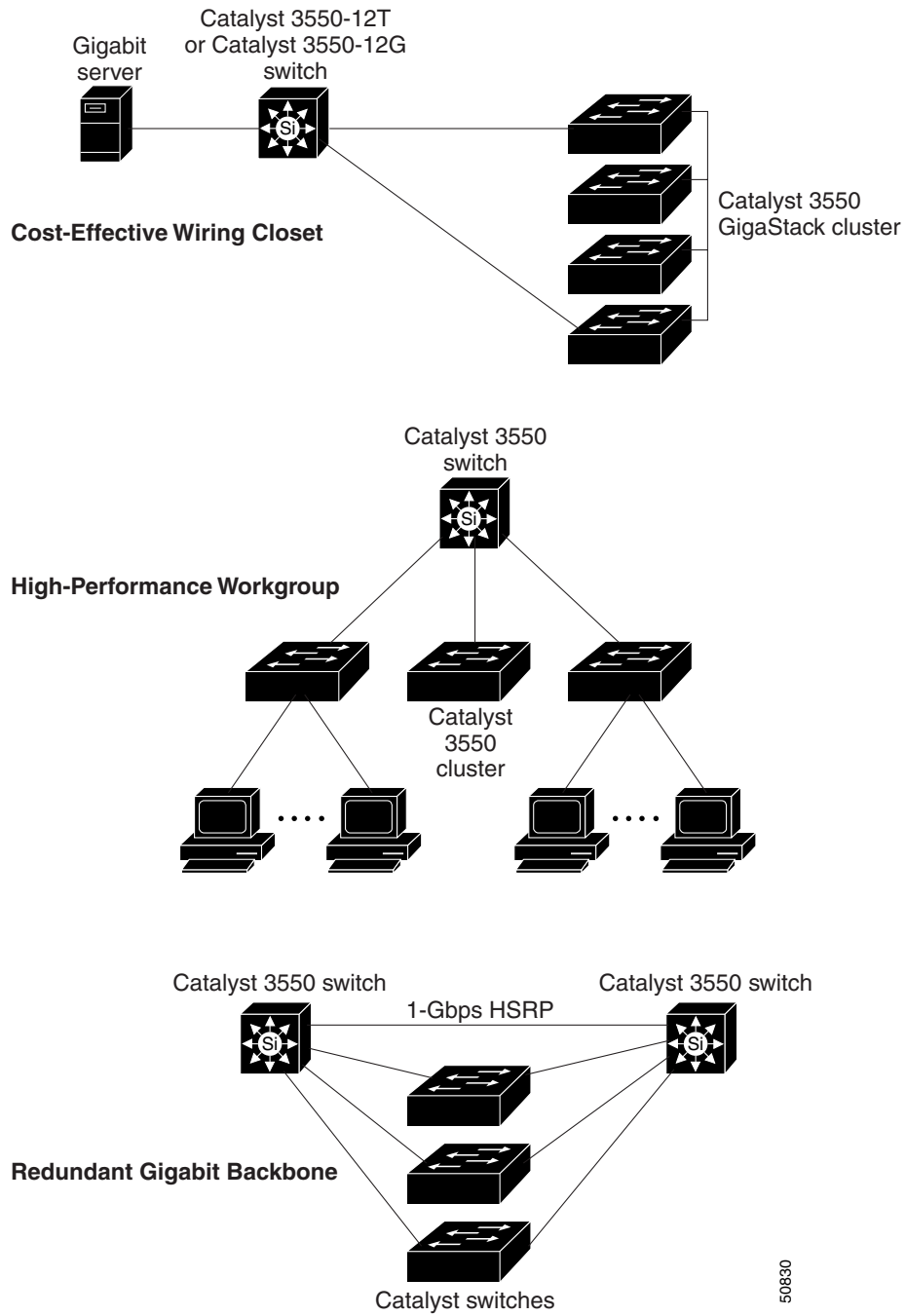
- **High-performance workgroup**—For users who require high-speed access to network resources, you can use Catalyst 3550 switches in the access layer to provide Gigabit Ethernet to the desktop. To prevent congestion, use QoS DSCP marking priorities on these switches. For high-speed IP forwarding at the distribution layer, connect the Catalyst 3550 switches in the access layer to a Gigabit multilayer switch in the backbone, such as the Catalyst 3550 multilayer switch. Use Gigabit connections between the switches in the access layer and the backbone switch.

Each switch in this configuration provides users with a dedicated 1-Gbps connection to network resources in the backbone. Compare this with the switches in a GigaStack configuration, where the 1-Gbps connection is shared among the switches in the stack. Using these Gigabit GBIC modules also provides flexibility in media and distance options:

- 1000BASE-SX GBIC: fiber-optic connections of up to 1804 ft (550 m)
  - 1000BASE-LX/LH GBIC: fiber-optic connections of up to 32,808 ft (10 km)
  - 1000BASE-ZX GBIC: fiber-optic connections of up to 328,084 ft (100 km)
  - 1000BASE-T GBIC: copper connections of up to 328 ft (100 m)
- **Redundant Gigabit backbone**—Using HSRP, you can create backup paths between two Catalyst 3550 multilayer switches to enhance network reliability and load balancing for different VLANs and subnets. Using HSRP also provides faster network convergence if any network failure occurs. You can connect the Catalyst switches, again in a star configuration, to two Catalyst 3550 multilayer backbone switches. If one of the backbone switches fails, the second backbone switch preserves connectivity between the switches and network resources.

The Catalyst 2950T-24 and Catalyst 2924M XL in this configuration are connected to the backbone switches through 1000BASE-T connections.

Figure 1-1 Example Configurations



## Small to Medium-Sized Network Using Mixed Switches

Figure 1-2 shows a configuration for a network of up to 500 employees. This network uses Catalyst 3550 multilayer switches to aggregate up to ten wiring closets through high-speed uplinks. For network reliability and load balancing, this network includes two routers and two Catalyst 3550 multilayer switches, all with HSRP enabled. This ensures connectivity to the Internet, WAN, and mission-critical network resources if one of the routers or Catalyst 3550 multilayer switches fails.

The wiring closets have a mix of switches such as the Catalyst 3550, Catalyst 2950, Catalyst 3500 XL, Catalyst 2900 XL, Catalyst 1900, and Catalyst 2820 switches. These switches are connected to workstations, Cisco IP Phones, and local servers. You can cluster these switches into multiple clusters, as shown, or into a single cluster. You can manage a cluster through the IP address of its primary and secondary command switches, regardless of the geographic location of the cluster members.

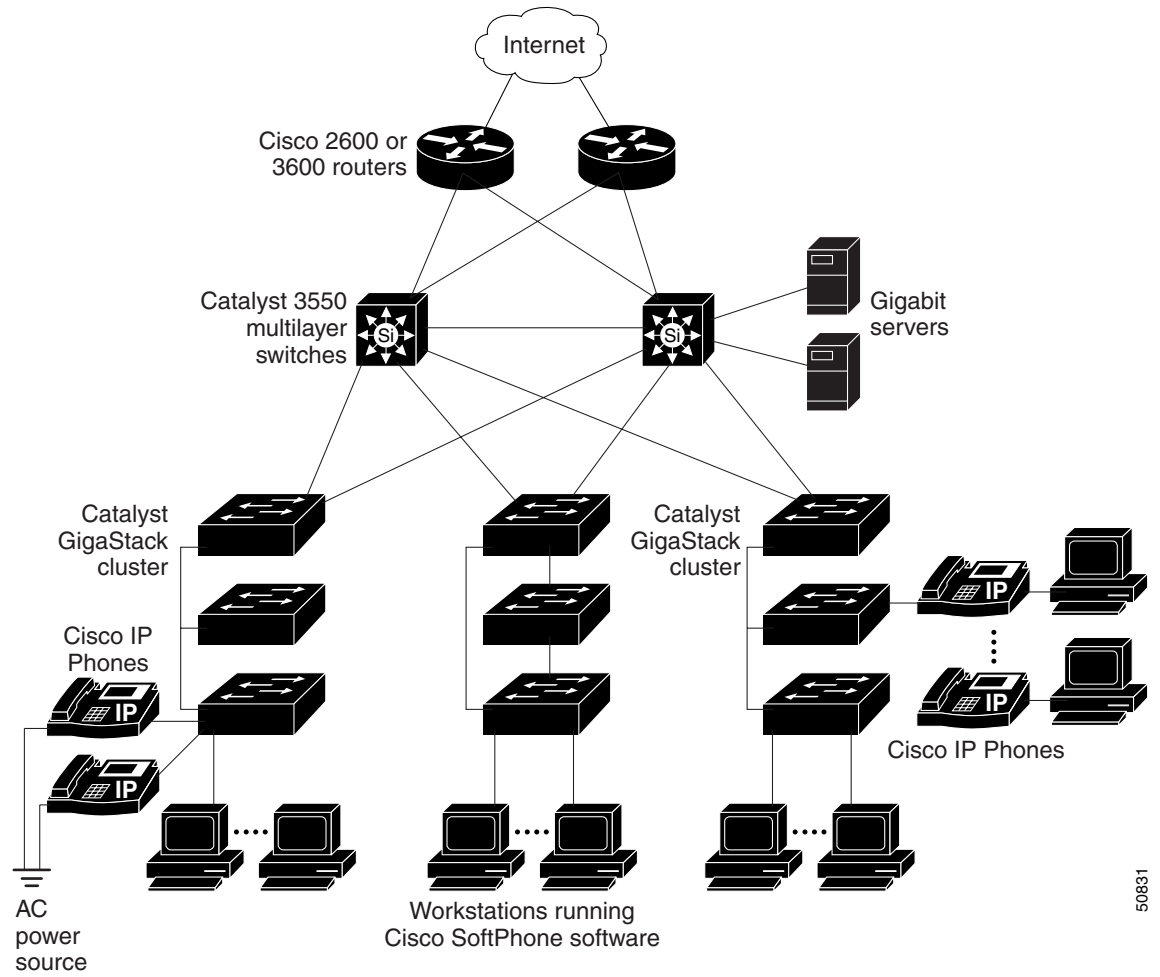
This network uses VLANs to segment the network logically into well-defined broadcast groups and for security management. Data and multimedia traffic are configured on the same VLAN. Voice traffic from the Cisco IP Phones are configured on separate VVIDs. You can have up to four VVIDs per wiring closet. If data, multimedia, and voice traffic are assigned to the same VLAN, only one VLAN can be configured per wiring closet. For any switch port connected to Cisco IP Phones, 802.1p/Q QoS gives voice traffic forwarding priority over data traffic.

When an end station in one VLAN needs to communicate with an end station in another VLAN, a router or multilayer switch routes the traffic to the appropriate destination VLAN. In this network, the Catalyst 3550 multilayer switches provide inter-VLAN routing. VLAN access control lists (VLAN maps) on the Catalyst 3550 switches provide intra-VLAN security and prevent unauthorized users from accessing critical pieces of the network.

In addition to inter-VLAN routing, the Catalyst 3550 multilayer switches provide QoS mechanisms such as DSCP priorities to prioritize the different types of network traffic and to deliver high-priority traffic in a predictable manner. If congestion occurs, QoS drops low-priority traffic to allow delivery of high-priority traffic.

With the Catalyst 3550 multilayer switches providing inter-VLAN routing and other network services, the routers are left to focus on firewall services, Network Address Translation (NAT) services, voice-over-IP (VoIP) gateway services, and WAN and Internet access.

Figure 1-2 Catalyst 3550 Switches in a Collapsed Backbone Configuration



50831

## Large Network Using Only Catalyst 3550 Switches

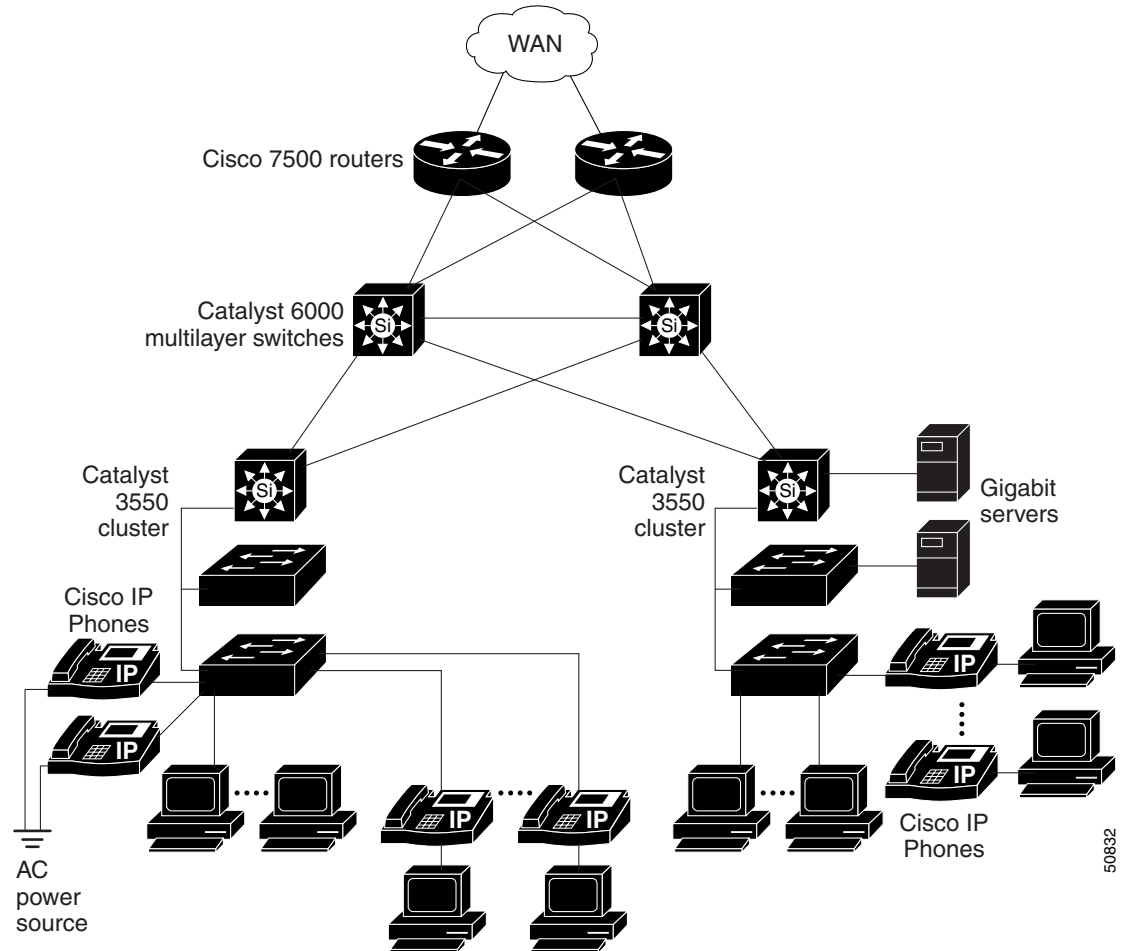
Switches in the wiring closet have traditionally been Layer 2-only devices, but as network traffic profiles evolve, switches in the wiring closet are increasingly employing multilayer services such as multicast management and traffic classification. [Figure 1-3](#) shows a configuration for a network exclusively using Catalyst 3550 multilayer switches in the wiring closets and a Catalyst 6000 switch in the backbone to aggregate up to ten wiring closets.

In the wiring closet, each Catalyst 3550 switch has IGMP snooping enabled to efficiently forward multimedia and multicast traffic. Also configured on each switch are QoS ACLs that either drop or mark nonconforming traffic based on bandwidth limits. VLAN maps provide intra-VLAN security and prevent unauthorized users from accessing critical pieces of the network. QoS features can limit bandwidth on a per-port or per-user basis. The switch ports are configured as either trusted or untrusted, indicating whether or not to trust the CoS values in received frames to be consistent with network policy. On trusted ports, QoS uses received CoS values. On untrusted ports, QoS replaces received CoS values with the port CoS value or with the values specified in the QoS ACLs. You also can configure the ports to trust the IP precedence TOS and DSCP priorities for traffic traversing the LAN/WAN and Internet/intranet boundaries.

Within each wiring closet is a Catalyst 3550 multilayer switch for inter-VLAN routing. These switches provide proxy ARP services to determine IP and MAC address mapping, thereby removing this task from the routers and lessening this type of traffic on the WAN links. These switches also have redundant uplink connections to the backbone switches, with each uplink port configured as a trusted routed uplink to provide faster convergence in case of an uplink failure.

The routers and Catalyst 6000 multilayer backbone switches have HSRP enabled for load balancing and redundant connectivity to guarantee mission-critical traffic.

Figure 1-3 Catalyst 3550 Switches in the Wiring Closets and Backbone Configuration



50832

